QUICK START GUIDE

Cisco ASA 5580

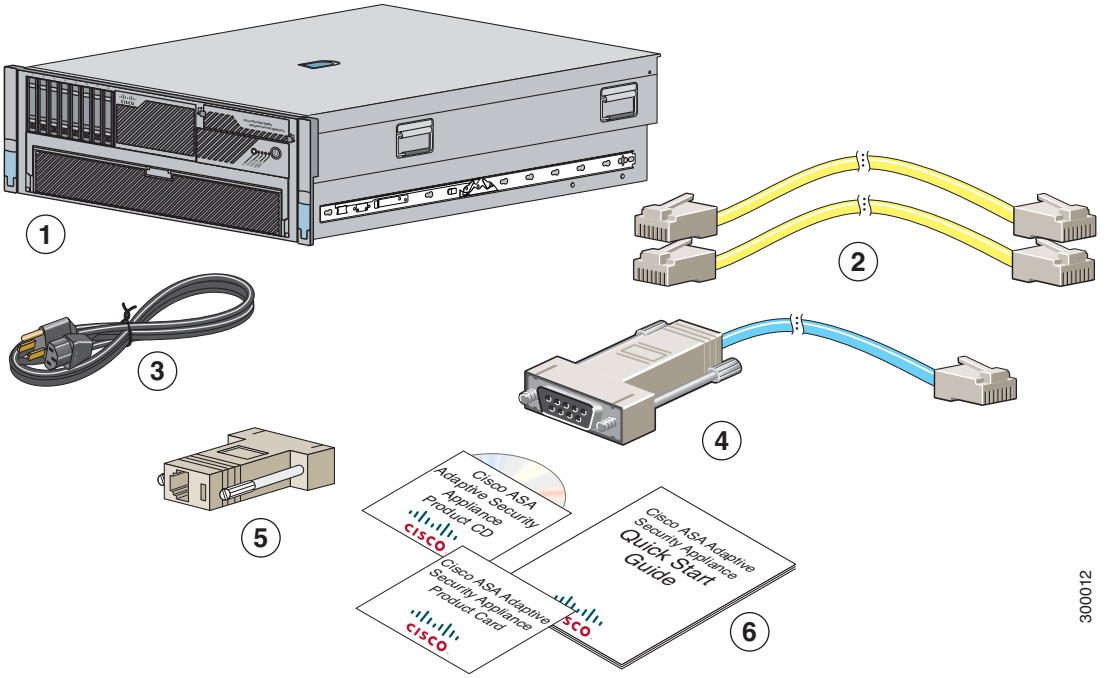
Regulatory Compliance and Safety Information

Read the safety warnings in the Regulatory Compliance and Safety Information (RCSI), and follow proper safety procedures when performing the steps in this guide. See http://www.cisco.com/go/asadocs for links to the RCSI and other documents.

Revised: January 30, 2012, 78-20726-01

1 Verifying the Package Contents

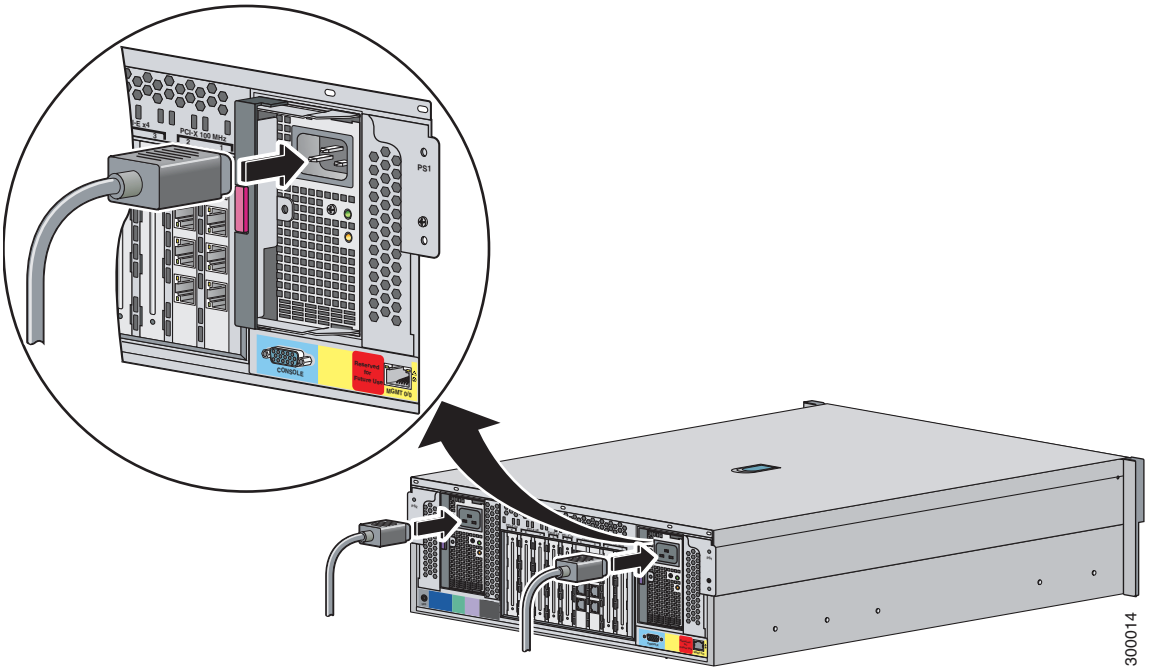
Verify the contents of the packing box to ensure that you have received all items necessary to install your ASA.



1	ASA 5580 Chassis	**2**	2 Yellow Ethernet Cables
3	Power Cable (US Shown)	**4**	Blue Console Cable PC Terminal Adapter
5	RJ-45 to DB-9 Adapter	**6**	Documentation and Software CD
	Not shown: Rail System Kit		

2 Powering On the ASA

Step 1 Attach the power cable to the back of the ASA. If you have redundant power supplies, you must connect both power cables to the back of the chassis.



Step 2 Connect the power cable(s) to the electrical outlets.

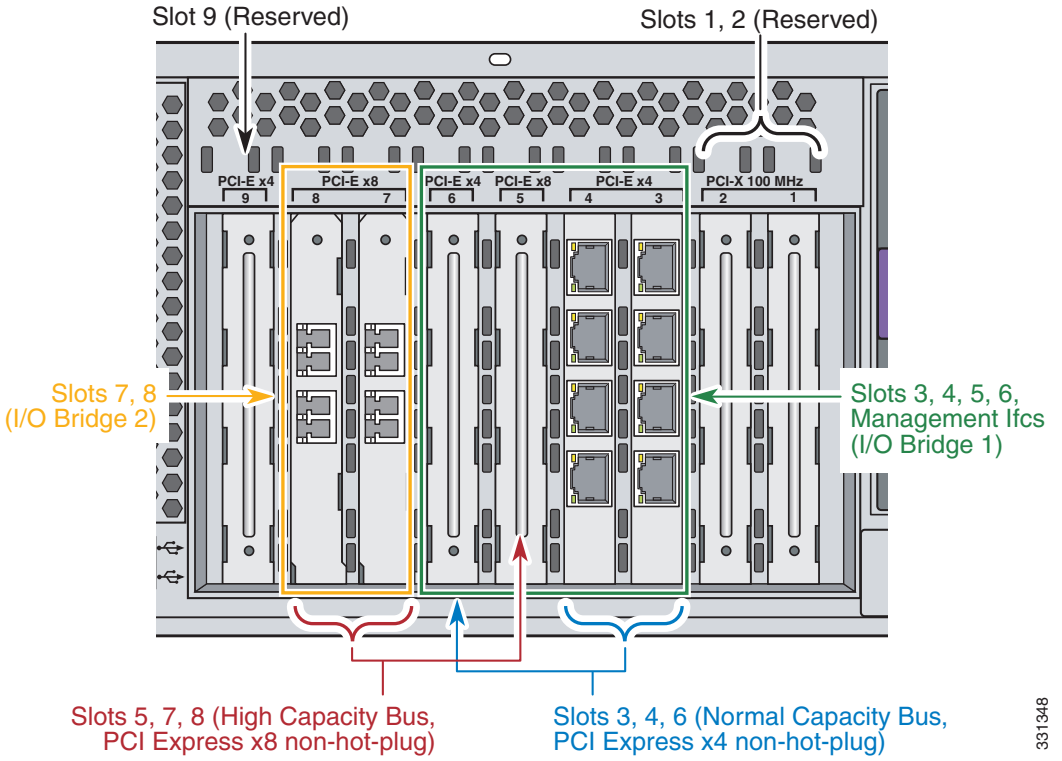
Step 3 Power on the ASA.

Step 4 Check the Power LED on the front of the ASA; if it is solid green, the device is powered on.

Step 5 Check the System LED on the front of the ASA; after it is solid green, the system has passed power-up diagnostics.

3 Maximizing Throughput

Refer to the following illustration when planning your network for maximum throughput.



- You should use the high-capacity bus slots (5, 7, 8) for 10-Gigabit Ethernet adapters; other adapters can be placed in any slot.
- Distribute traffic on the I/O bridges using the following best practices:
  - Have equal amounts of traffic on both I/O bridges.
  - Keep traffic flow within the same I/O bridge.

  For example, the ideal traffic distribution would be:

  a. Half the traffic stays on slots 7 and 8.

  b. The other half of the traffic stays on slots 3 through 6.

  Steps a and b achieve both best practices above. If you cannot achieve both practices, then you should prefer the first best practice: have equal amounts of traffic on both I/O bridges.

See the Hardware Installation Guide for more information about maximizing throughput on the ASA 5580.

4 Connecting Interface Cables and Verifying Connectivity

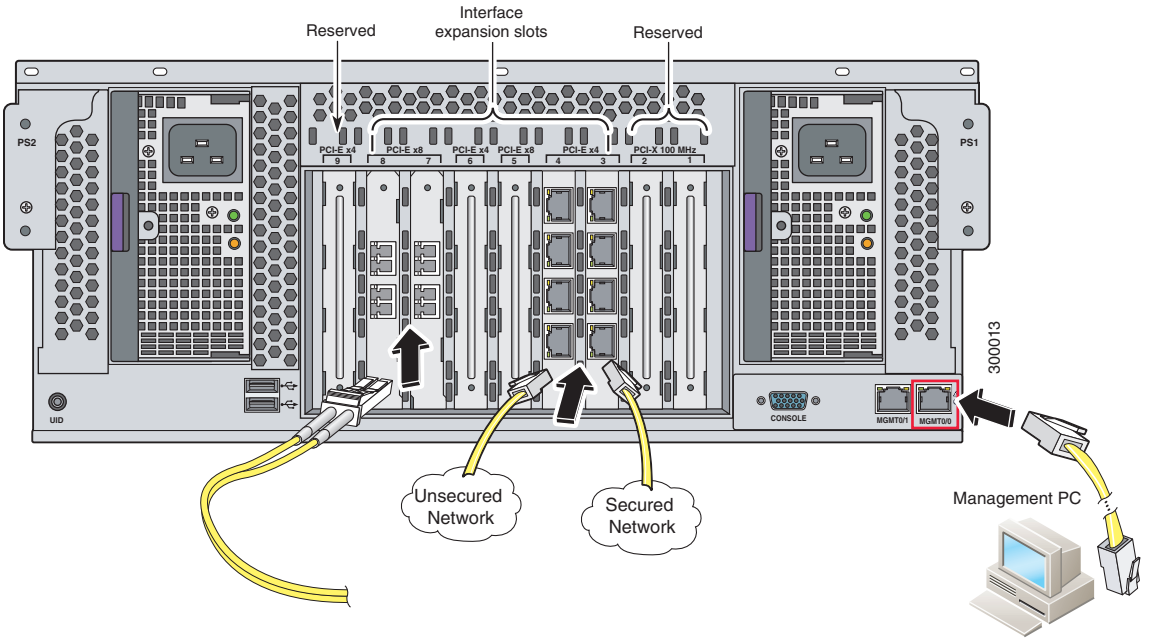
Step 1 Connect to the Management 0/0 interface so that you can use ASDM to manage the ASA. You can connect the PC directly with an Ethernet cable, or connect the PC and the ASA to the same management network. Make sure the PC is configured to obtain an IP address using DHCP.

The ASA 5580 has 2 management interfaces (Management 0/0 and Management 0/1); however, only Management 0/0 is configured for use.

If you want to use the CLI, connect your PC to the console port, and see the CLI configuration guide for more information.

Step 2 Connect your networks to the appropriate ports.

The ASA 5580 has nine expansion slots. Slots 3 through 8 support PCI Express network interface adapters. Slots 1, 2, and 9 are reserved. Your exact configuration depends on the configuration you purchased.



Step 3 Check the LINK/ACT indicators to verify interface connectivity.

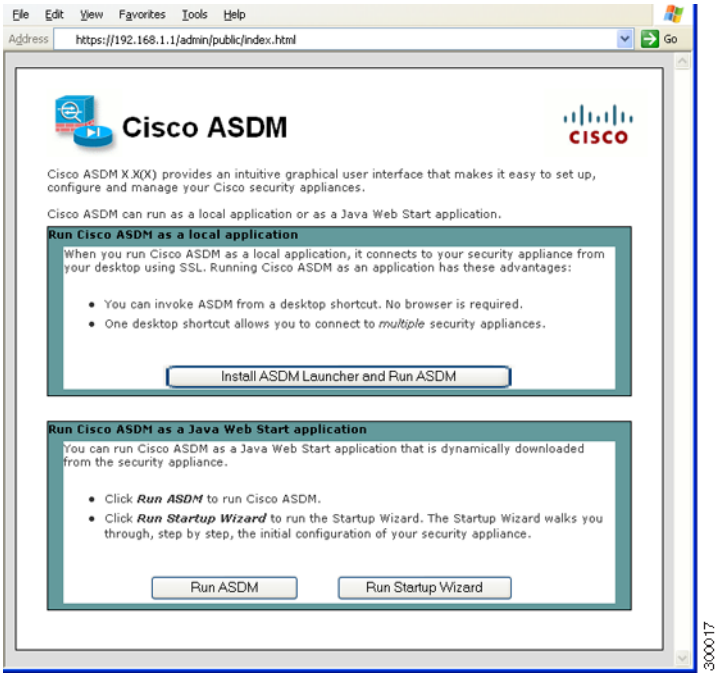
5 Launching ASDM

The ASA ships with a default configuration that enables ASDM connectivity to the Management 0/0 interface. Using ASDM, you can use wizards to configure basic and advanced features. ASDM is a graphical user interface that allows you to manage the ASA from any location by using a web browser.

See the ASDM release notes on Cisco.com for the requirements to run ASDM.

Step 1 On the PC connected to the ASA, launch a web browser.

Step 2 In the Address field, enter the following URL: **https://192.168.1.1/admin**. The Cisco ASDM web page appears.



Step 3 Click **Run Startup Wizard**.

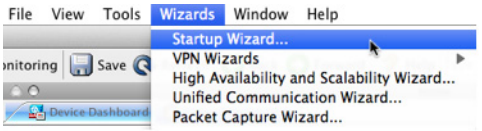
Step 4 Accept any certificates according to the dialog boxes that appear. The Cisco ASDM-IDM Launcher appears.

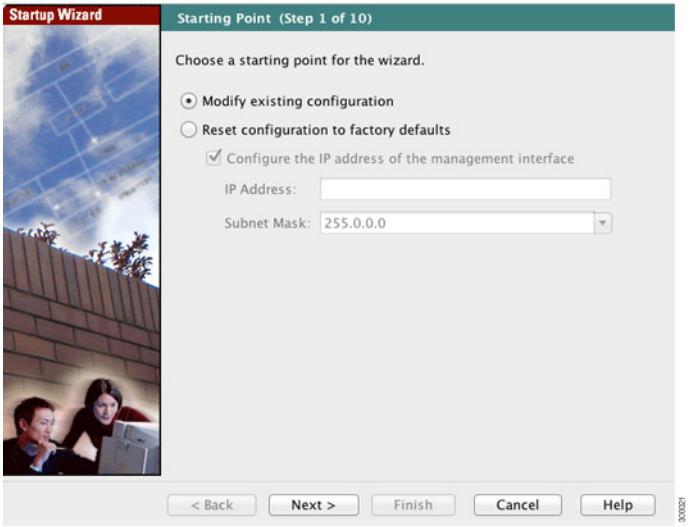
Step 5 Leave the username and password fields empty, and click **OK**. The main ASDM window appears and the Startup Wizard opens.

6 Running the Startup Wizard

Run the **Startup Wizard** to modify the default configuration so that you can customize the security policy to suit your deployment. Using the startup wizard, you can set the following:

- Hostname
- Domain name
- Administrative passwords
- Interfaces
- IP addresses
- Static routes
- DHCP server
- Network address translation rules
- and more...





Step 1 If the wizard is not already running, in the main ASDM window, choose **Wizards > Startup Wizard**.

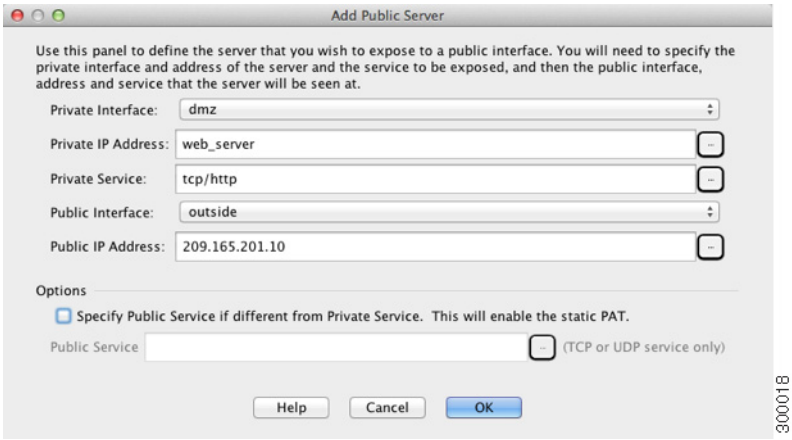
Step 2 Follow the instructions in the Startup Wizard to configure your ASA.

Step 3 While running the wizard, you can accept the default settings or change them as required. (For information about any wizard field, click **Help**.)

7 (Optional) Allowing Access to Public Servers Behind the ASA

ASA 8.2 and Later

The Public Server pane automatically configures the security policy to make an inside server accessible from the Internet. As a business owner, you might have internal network services, such as a web and FTP server, that need to be available to an outside user. You can place these services on a separate network behind the ASA, called a demilitarized zone (DMZ). By placing the public servers on the DMZ, any attacks launched against the public servers do not affect your inside networks.



Step 1 In the main ASDM window, choose **Configuration > Firewall > Public Servers**. The Public Server pane appears.

Step 2 Click **Add**, then enter the public server settings in the Add Public Server dialog box. (For information about any field, click **Help**.)

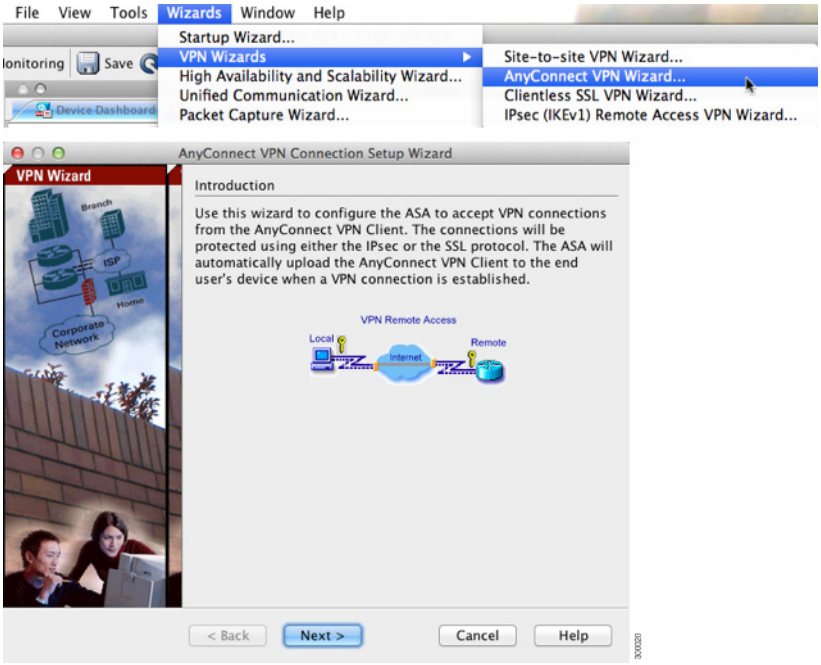
Step 3 Click **OK**. The server appears in the list.

Step 4 Click **Apply** to submit the configuration to the ASA.

8 (Optional) Running VPN Wizards

You can configure VPN using the following wizards:

- Site-to-Site VPN Wizard—Creates an IPsec site-to-site tunnel between two ASAs.
- AnyConnect VPN Wizard—Configures SSL VPN remote access for the Cisco AnyConnect VPN client. AnyConnect provides secure SSL connections to the ASA for remote users with full VPN tunneling to corporate resources. The ASA policy can be configured to download the AnyConnect client to remote users when they initially connect via a browser. With AnyConnect 3.0 and later, the client can run either the SSL or IPsec IKEv2 VPN protocol.
- Clientless SSL VPN Wizard—Configures clientless SSL VPN remote access for a browser. Clientless, browser-based SSL VPN lets users establish a secure, remote-access VPN tunnel to the ASA using a web browser. After authentication, users access a portal page and can access specific, supported internal resources. The network administrator provides access to resources by users on a group basis. ACLs can be applied to restrict or allow access to specific corporate resources.
- IPsec (IKEv1) Remote Access VPN Wizard—Configures IPsec VPN remote access for the Cisco IPsec client.



Step 1 In the main ASDM window, choose **Wizards > VPN Wizards,** then choose one of the following:

- **Site-to-Site VPN Wizard**
- **AnyConnect VPN Wizard**
- **Clientless VPN Wizard**
- **IPsec (IKEv1) Remote Access VPN Wizard**

Step 2 Follow the wizard instructions. (For information about any wizard field, click **Help**.)

9 (Optional) Running Other Wizards in ASDM

You can optionally run the following additional wizards in ASDM:

- High Availability and Scalability Wizard

  Configure active/active or active/standby failover, or VPN cluster load balancing.

- Unified Communications Wizard

  Configure a proxy on the ASA for remote access or business-to-business communications. (Special licenses may apply. See the CLI configuration guide for information about ASA licensing.)

- Packet Capture Wizard

  Configure and run packet capture. The wizard will run one packet capture on each of the ingress and egress interfaces. After capturing packets, you can save the packet captures to your PC for examination and replay in the packet analyzer.

10 Advanced Configuration

To continue configuring your ASA, see the documents available for your software version at:

http://www.cisco.com/go/asadocs

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices**.

78-20726-01